(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－252177

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.^{6}	識別記号	ＦＩ	
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｚ
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ　1/00	Ｆ
7/00		7/00	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１

審査請求　未請求　請求項の数４　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－50527

(22)出願日　平成10年(1998) ３月３日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　石井　眞
東京都品川区北品川６丁目７番35号ソニー株式会社内

(74)代理人　弁理士　田辺　恵基

(54)【発明の名称】　暗号化装置及び暗号化方法

(57)【要約】
【課題】複数の素材データを同時に暗号化処理し得る暗号化装置及び暗号化方法を実現し難かつた。
【解決手段】入力する素材データを必要に応じて暗号化する暗号化装置において、素材データを、暗号化するか否かを表す第１の暗号化情報を付加して所定単位でパケツト化するパケツト化手段と、パケツト化された素材データを、パケツト毎に対応する第１の暗号化情報に基づいて必要に応じて暗号化する暗号化手段とを設けるようにした。また入力する素材データを必要に応じて暗号化する暗号化方法において、素材データを、暗号化するか否かを表す第１の暗号化情報を付加して所定単位でパケツト化する第１のステツプと、パケツト化された素材データを、パケツト毎に対応する第１の暗号化情報に基づいて必要に応じて暗号化する第２のステツプとを設けるようにした。

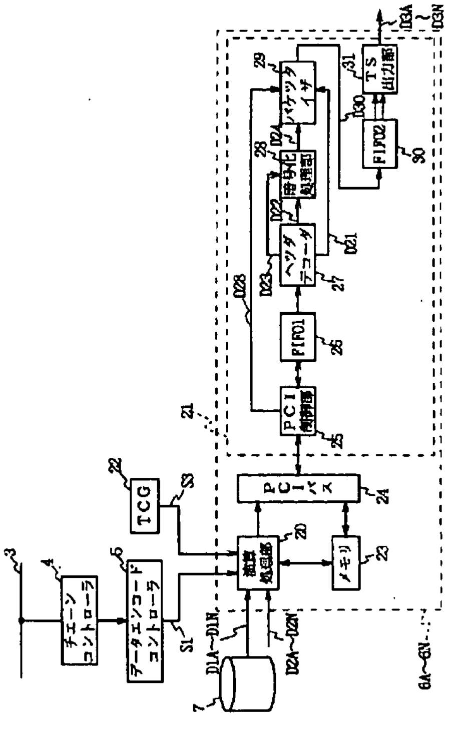

図２　放送素材エンコード処理用のデータエンコーダの構成

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Table of Contents] This invention is explained in order of the following.
[0002] The technical problem which technical field Prior-art invention to which invention belongs tends to solve (drawing 5)
The means for solving a technical problem (drawing 1 - drawing 5)
The data-broadcasting structure of a system by the gestalt of gestalt (1) book implementation of implementation of invention (drawing 1 and drawing 5)
(2) A data encoders [6A-6N] configuration (drawing 1 - drawing 3 , and drawing 5)
(3) The detail configuration of the encryption processing section 28 (drawing 2 - drawing 5)
(4) Actuation and effectiveness (drawing 1 - drawing 5) of the gestalt of this operation
(5) The gestalt of other operations (drawing 1 - drawing 5)
Effect of the invention [0003]
[Field of the Invention] This invention is applied to the data encoder of the transmitting side in the data-broadcasting system using a satellite, concerning encryption equipment and the encryption approach, and is suitable.
[0004]
[Description of the Prior Art] In recent years, in the broadcast system using a satellite, many channelization is progressing by compression processing of image voice data in which MPEG 2 (Moving Picture ExpertsGroup Phase2) was used.
[0005] And in such multi-channel digital broadcast, various data broadcast services, such as news service, and music service, the Internet service, are

carried out, using the fast transmission engine performance (it is a maximum of 30 [Mbps] by the case of 27 [MHz]) of the transponder carried in the satellite.

[0006]

[Problem(s) to be Solved by the Invention] by the way -- the Internet -- data -- a TCP/IP (Transmission Control Protocol/Internet Protocol) format -- therefore, it is transmitted by the signal aspect by which the IP header HD 1 was added to the head like drawing 5 (A).

[0007] on the other hand, the DVB-SI (Digital Video Broadcasting-Service Information) format which is the specification for data broadcasting among the digital satellite broadcasting standards of Europe in data broadcasting -- therefore, drawing 5 (G) -- like -- data -- 184 It is divided per cutting tool and transmitted by the signal aspect to which 4 bytes of TS (Transport Stream) header HD 6 was added, respectively and which was formed into TS packet.

[0008] Incidentally, as shown in drawing 5 (H), the sink cutting tool data D40 (0x47 immobilization) for detecting the head of a packet at the head are stored in the TS header HD 6. the middle -- every channel -- and the PID (Packet Identification) data D41 which become by the 13-bit identification information of a value which is different also by the same channel for every broadcast material, such as an image, Japanese voice, foreign language voice, control information, and text information, are stored. Moreover, the counter value (continuing tee counter value) data D42 with which the TS packet expresses the thing of what position of the broadcast material it is are stored in the tail end of the TS header HD 6.

[0009] Therefore, in carrying out data broadcasting of the data which are flowing the Internet top, for example, it is necessary to change the format into a DVB-SI format from a TCP/IP format, and uses the data encoder of a personal computer configuration of such format conversion processing in the former, and it is line intermediary **** by software processing.

[0010] However, the problem which needs great time amount for data processing, and TS packet-ized processing and encryption processing of redundancy data (CRC (Cyclic Redundancy Check) data) required for the error check of data transmission added at the time of data broadcasting, and cannot perform such format conversion processing easily due to real time for this reason when software processing performs such format conversion processing is ******. Moreover, the problem which needs a thing expensive at high speed as a data encoder in order to perform such format conversion processing on real time, and also makes the configuration and program complicated is ******.

[0011] As one approach for solving this trouble, among the above format conversion processings, while carrying out software processing of the attached processing of a header with little ****** etc. therefore, according to software, the large approach of a load which is made to carry out hardware processing of data processing, TS packet-ized processing, encryption processing of CRC data, etc., for example can be considered for software.

[0012] According to this approach, since data processing, TS packet-ized processing, encryption processing of CRC data, etc. can be performed on real time, there is an advantage which can perform efficiently format conversion processing to the DVB-SI format from a TCP/IP format on real time.

[0013] And if one broadcast material cannot be processed in one data encoder in this case but format conversion of two or more broadcast materials of a broadcast schedule can be carried out to the same time amount at coincidence (to time sharing), it will be thought that the configuration of the transmitting side in the part it becomes unnecessary to form a data encoder for every broadcast material, and a data-broadcasting system is simplified, and it can make it possible to build this cheaply.

[0014] However, in order to do in this way, it is necessary to build a data encoder so that encryption (to time sharing) processing of two or more broadcast materials can be carried out at coincidence, and the device which enables it to switch efficiently the processing in the case of updating the on-off control of whether for that to encipher for every broadcast material in the interior of a data encoder and the key of encryption is needed.

[0015] This invention was made in consideration of the above point, and tends to propose the encryption equipment and the encryption approach of carrying out encryption processing of two or more material data at coincidence.

[0016]

[Means for Solving the Problem] In order to solve this technical problem, a packet-ized means to add the 1st encryption information which means whether material data are enciphered in encryption equipment in this invention, and to packet-ize per predetermined, and an encryption means to encipher the packet-ized material data if needed based on the 1st encryption information which corresponds for every packet were established.

[0017] As a result, it is controllable by this encryption equipment per packet whether it enciphers or not.

[0018] Moreover, in the encryption approach, the 1st step which adds the 1st encryption information showing whether material data are enciphered, and is

packet-ized per predetermined, and the 2nd step which enciphers the packet-ized material data if needed based on the 1st encryption information which corresponds for every packet were prepared.
[0019] As a result, according to this encryption approach, it is controllable per packet whether it enciphers or not.
[0020]
[Embodiment of the Invention] About a drawing, the gestalt of 1 operation of this invention is explained in full detail below.
[0021] (1) In data-broadcasting structure-of-a-system drawing 1 by the gestalt of this operation, 1 shows the data-broadcasting system by the gestalt of this operation as a whole, and a minute of broadcast schedule information will be given to chain KONTORA 4 several days through LAN (Local Area Network)3 from the transmitting system controller 2.
[0022] Based on the broadcast schedule information supplied, the chain controller 4 generates schedule information, such as a broadcast day of a broadcast material, broadcasting hours, ID, and a flow rate (process speed), and gives this to the data encoding controller 5.
[0023] If the data encoding controller 5 has managed the broadcasting hours of each broadcast material based on the schedule information supplied and consists of broadcast time of day of one of broadcast materials before predetermined time By sending out a control signal S1 to the data encoders 6A-6N with which it corresponds of the data encoders 6A-6N for two or more broadcast material encoding processings, and controlling this Data D1 A-D1N of a corresponding broadcast material is made to read to the record playback section 7, or data D2 A-D2N of a corresponding broadcast material is made to incorporate from the outside (for example, Internet).
[0024] In this case, beforehand, data D1 A-D1N of two or more broadcast materials of a broadcast schedule is file-ized by the record playback section 7, and is stored in it by the signal aspect of a DVB-SI format, a TCP/IP format or a section format like drawing 5 (B) either. Moreover, data D2 A-D2N from the outside is given in a TCP/IP format.
[0025] Incidentally in a section format of drawing 5 (B), sequential addition of the control header HD 4 including whether it is enciphered as the key data D10 showing the value of the key at the time of enciphering it as the section header HD 3 which comes to contain the information which specifies the MAC (Media Access Contrrol) header HD 2 and the candidate for receiving at the head of the data of a TCP/IP format or it does not carry out, and control information is carried out.

[0026] In this way, when the signal aspect of the reproduced broadcast material which is supplied from the record playback section 7 is a DVB-SI format, the data encoders 6A-6N While sending out to a multiplexer 8 on schedule by setting this to TS packet data D2 A-D2N as it is When the signal aspect of the broadcast material supplied from the record playback section 7 is a TCP/IP format or a section format, and when a broadcast material is incorporated from the outside After changing this into a DVB-SI format, it sends out to a multiplexer 8 on schedule as TS packet data D3 A-D3N.
[0027] Moreover, at this time, data encoder 6R for control data encoding processing sends out obtained TS packet data D3R to a multiplexer 8, after forming into TS packet the control data D4 supplied from the control data feed zone which is not illustrated.
[0028] In a multiplexer 8, TS packet data D3 A-D3N supplied, respectively from each data encoders 6A-6N and 6R and D3R are multiplexed, and the obtained multiplexing data D5 are sent out to the QPSK (Quadrature Phase Shift Keying) modulator 9.
[0029] And after adding error correction code data to the multiplexing data D5 supplied, while it performs 4 phase phase modulation (QPSK) processing, the QPSK modulator 9 this It sends out to the output amplifier which does not illustrate the obtained sending signal S2, and after making predetermined signal processing which carries out the frequency shift of the IF signal of 70 [MHz] 14 [GHz] perform in the output amplifier concerned, this is sent out towards a satellite 11 through the transmitting-side antenna 10.
[0030] This sending signal S2 is received by the receiver 13 through the corresponding transponder and the corresponding receiving-side antenna 12 in a satellite 11 one by one after this in this way. And this is restored and a receiver 13 displays the image and alphabetic character based on data D1 A-D1N and D2 A-D2N which was restored on a monitor while extracting data D1 A-D1N of the broadcast material of the channel specified by the user contained in the sending signal S2 which received, and D2 A-D2N, and it makes voice output from a loudspeaker.
[0031] Thus, in this data-broadcasting system 1, in the transmitting side, while data D1 A-D1N of the broadcast material for two or more channels and D2 A-D2N are multiplexed and it can send out, in the receiving side, it is made as [listen / to the broadcast material for which a user asks out of these broadcast material / it / choose, view and].
[0032] In addition to this configuration, in the case of this data-broadcasting system 1, the data encoding controller 5 is made as [give / the material ID of

two or more broadcast materials which should be broadcast to coincidence if needed to each data encoders 6A-6N etc. / as a control signal S1].

[0033] And each data encoders 6A-6N are based on two or more materials ID which may be based on the control signal S1 supplied. Data D1 A-D1N of these materials ID and each broadcast material which corresponds, respectively, While making the record playback section 7 read D2 A-D2N to time sharing or incorporating from the outside When data D1 A-D1N of these broadcast material and D2 A-D2N are a section format or a TCP/IP format, the data D1 A-D1N concerned, It is made as [send / to a multiplexer 8 / form TS packet and], performing on-off control of encryption of D2 A-D2N for every broadcast material, renewal of the key of encryption, etc.

[0034] Thereby, in this data-broadcasting system 1, data D1 A-D1N of two or more broadcast materials and D2 A-D2N can be TS-packet--ization-processed to coincidence in each data encoders 6A-6N, and it is made as [constitute / as the whole system / in this way / it / simply].

[0035] (2) a data encoders [6A-6N] configuration -- as here shows each data encoders 6A-6N for broadcast material encoding processing to drawing 2 , it has the data-processing section 20 of a microcomputer configuration, and the encoder board 21 of a hardware configuration, and input into the data-processing section 20 the control signal S1 supplied from the data encoding controller 5, and the time code signal S3 supplied from the time code generator 22.

[0036] Moreover, that information (this is hereafter called format information) whose signal aspect of each [these] broadcast material is any of a DVB-SI format, a TCP/IP format, and a section format, respectively is also given to the data-processing section 20 as a control signal S1 from the data encoding controller 5 with the information on the material ID of each broadcast material which should be broadcast etc. at this time.

[0037] The data-processing section 20 is based on the control signal S1 and the time code signal S3 which are supplied in this way. The record playback section 7 is made to reproduce data D1 A-D1N which corresponds if it consists of specified broadcast time of day of a broadcast material before predetermined time to time sharing if needed. Or data D2 A-D2N of the broadcast material supplied is incorporated from the outside to time sharing if needed. When the data format is a DVB-SI format, while these are stored in memory 23 as they are When the data D1 A-D1N concerned and D2 A-D2N are section formats of drawing 5 (B), by removing the control header HD 4 and the key header D10, it changes into the data D12 of a section format of drawing 5 (C), and stores in memory 23.

[0038] Moreover, data D1 A-D1N of the broadcast material which the record playback section 7 was made to reproduce the data-processing section 20 to time sharing if needed, or was incorporated from the exterior to time sharing if needed, When the data format of D2 A-D2N is a TCP/IP format This is stored in memory 23 after changing into the data D12 of a section format by carrying out sequential addition of the MAC header HD 2 and the section header HD 3 like drawing 5 (C) at the head of the data D1 A-D1N concerned and D2 A-D2N by software processing.

[0039] in addition, each data D1 A-D [in / to drawing 3 / memory 23]1 -- the data format of N and D12 is shown. N and D12 make one unit the amount of data which is read from the record playback section 7 to time sharing, or is incorporated by time sharing from the exterior. clear also from this drawing 3 -- as -- each data D1 A-D1 -- Sequential storing is carried out in each division record section (cluster) divided into every 4[Kbit[in memory 23]] after having been packet-ized by the magnitude of under 4 [Kbit] by adding the control header HD 5 to the head for every unit, respectively. Incidentally data D1 A-D1N of each broadcast material is stored in the record playback section 7 in the condition of having been beforehand divided into the magnitude corresponding to such packet-izing.

[0040] It is based on the various information given to the control header HD 5 from the data encoding controller 5 (drawing 2) at this time or it is contained in the control header HD 4 (drawing 5 (B)). The 10-bit text word data D14 showing the data length of the packet, data D1 A-D1 in this packet -- with the 1-bit EN (Encrypt or Not) data D15 which express ("0") for whether it is enciphering N and D12 ("1") The 1-bit KA (Key Avail) data D16 which express ("0") for whether it is updating the key at the time of enciphering to a new thing ("1"), data D1 A-D1 in this packet -- the 13 bits PID data D17 showing the value of PID which should be given in case N and D12 are formed into TS packet, and the 12-bit reserve data D18 are stored. It is 128, when enciphering data D1 A-D1N in this packet, and D12 to the control header HD 5 and updating a key to it furthermore at the time of a parenthesis (EN=1, KA=1). The key data D19 for a bit are stored.

[0041] and such each data D1 A-D1 that was packet-ized and was stored in memory 23 -- N and D12 are read one by one to the basis of control of the data-processing section 20 by the PCI control section 25 of the encoder board 21 per cluster (namely, packet unit) through the PCI (Peripheral Component Interconnect) bus 24 after this. Moreover, that information whose signal aspect of each [these] broadcast material is any of a DVB-SI format and a section format, respectively is also given to the PCI control section 25 through the data-processing section 20 from the data encoding controller 5 at this time.

[0042] In this way, the PCI control section 25 gives this to the header decoder 27 through FIFO (First-In First-Out)26, when the data format of the broadcast material given through PCI bus 24 based on this format information is a DVB-SI format. And after removing the control header HD 5 (drawing 3) for data D1 A-D1N of this broadcast material in the header decoder 27 after this, It gives TS output section 31, without also performing what signal processing through the encryption processing section 28, PAKETSUTAIZA 29, and FIFO30 one by one. After performing predetermined signal processing in the TS output section 31 concerned, it sends out to a multiplexer 8 (drawing 1) as above-mentioned TS packet data D3 A-D3N (drawing 1).

[0043] On the other hand, the PCI control section 25 gives this to the header decoder 27 through FIFO26, when the data format of the broadcast material given through PCI bus 24 is a section format.

[0044] At this time, while the header decoder 27 carries out sequential removal of the control header HD 5 from the data D12 of each broadcast material of the packet unit by which sequential supply is carried out It sends out to PAKETSUTAIZA 29 among the data D12 of the section format obtained by using a section header HD 3 and the MAC header HD 2 as the header data D21. After adding the padding data D20 which become in the IP data concerned like drawing 5 (D) about the IP header HD 1 and IP data by the dummy data for making it 8 bytes of integral multiple, it sends out to the encryption processing section 28 per above-mentioned packet as IP section data D22.

[0045] Moreover, the header decoder 27 extracts the EN data D15 and the KA data D16 which are contained in the control header HD 5 (drawing 3) of each packet, and the key data D19 (in the case of kA= "1"), and carries out sequential sending out per above-mentioned packet by making these into the header data D23 at the encryption processing section 28.

[0046] The encryption processing section 28 enciphers the IP section data D22 in the packet only corresponding to the case of EN= "1" based on the header data D23 of each packet by which sequential supply is carried out. At this time, while the encryption processing section 28 enciphers the IP section data D22 using the key data D19 given at the time of the encryption processing which is preceded in EN= "1" and KA= "0" The IP section data

D22 in the packet which corresponds based on the key data D19 given as header data D23 at this time in EN= "1" and KA= "1" are enciphered, and the obtained encryption data D24 are sent out to PAKETSUTAIZA 29.
[0047] The encryption data D24 with which PAKETSUTAIZA 29 is given from the encryption processing section 28, While generating the section data D25 as which it comes to encipher only the IP section data D22 as shown in drawing 5 (E) for every broadcast material by multiplexing the corresponding header data D21 given from the header decoder 27 Hardware processing generates the 32-bit CRC data D26 according to each section data D25, respectively, and the MAC frame data D27 are generated by adding these to the tail end of the section data D25 which corresponds like drawing 5 (F), respectively.
[0048] Moreover, PAKETSUTAIZA 29 is the MAC frame data D27 for every broadcast material of this like drawing 5 (G), respectively 184 While carrying out sequential division for every cutting tool Based on the PID data D28 (drawing 2) given from the PCI control section 25 at this time, sequential generation of 4 bytes of TS header HD 6 is carried out. It is these TS header HD 6, respectively 184 Corresponding data divided into the cutting tool (This is hereafter called division data) By adding to the head of D29, it TS-izes [packet-] and each obtained TS packet data D30 (drawing 2) is sent out to TS output section 31 through FIFO30.
[0049] In this way, this TS packet data D30 is sent out to a multiplexer 8 as above-mentioned TS packet data D3 A-D3N, after predetermined signal processing is performed in TS output section 31 after this.
[0050] Thus, in each data encoders 6A-6N, data D1 A-D1N of each broadcast material of the section format supplied or a TCP/IP format and D2 A-D2N are changed and outputted to TS packet data D3 A-D3N of a DVB-SI format, respectively.
[0051] (3) the detail configuration of the encryption processing section 28 -- as the encryption processing section 28 is shown in drawing 4 , it consists of encryption on-off control block 40 and encryption block 41, and input into the switch control section 42 and switch 43 of the encryption on-off control block 40 the header data D23 for every packet given from the header decoder 27 (drawing 2 R> 2) here.
[0052] at this time, the switch control section 42 separates the EN data D15, the KA data D16, and the key data D19 which are contained in the header data D23 by carrying out change control of the switch 43 based on the header data D23 supplied -- making -- these -- respectively -- the 1- of D-flip-flop circuit

configuration -- it is made to send out to the 3rd data storage attaching part 44A-44C moreover, the 1- the 3rd data storage attaching part 44A-44C carries out storage maintenance of the EN data D15, the KA data D16, or the key data D19 supplied, and gives this to the encryption control section 45 of the encryption block 41.

[0053] The IP section data D22 in each packet given from the header decoder 27 on the other hand are also given to 1st encryption section 47A through the encryption control section 45 while they are given to the head detecting element 46 of the encryption block 41. At this time, whenever the head detecting element 46 detects the head of the packet supplied and detects the head concerned, it sends out the head detecting signal S10 to the encryption control section 45.

[0054] based on the EN data D15 and the KA data D16 which are given from the 1st and 2nd data storage attaching parts 44A and 44B, the encryption control section 45 is the timing to which the head detecting signal S10 was given, and, in EN= "1" and KA= "1" (encryption and renewal of the key for encryption are carried out), enciphers the IP section data D22 -- as -- the 1- the 3rd encryption section 47A-47C is controlled.

[0055] Moreover, the encryption control section 45 stores data (these are hereafter called 1st and 2nd key data, respectively) D19A of two keys for the encryption which may be based on the key data D19 given from 3rd data storage attaching part 44C with this, and D19B in the 1st or 2nd register 48A and 48B which corresponds, respectively.

[0056] The IP section data D22 for one packet given to 1st encryption section 47A through the encryption control section 45 at this time in this way After encryption processing was carried out based on 1st key data D19A stored in 1st register 48A in the 1st encryption section 47A concerned, Encryption processing is carried out based on 2nd key data D19B stored in 2nd register 48B in 2nd encryption section 47B. After encryption processing is carried out based on 1st key data D19A stored in 1st register 48A in 3rd encryption section 47C after this, it is sent out to PAKETSUTAIZA 29 (drawing 2) of the next step as above-mentioned encryption data D24 through the output section 49.

[0057] On the other hand, the encryption control section 45 is the timing to which the head detecting signal S10 was given based on the EN data D15 and the KA data D16 which are given from the 1st and 2nd data storage attaching parts 44A and 44B. in the case of EN=1 and KA=0 (the key of encryption is not updated although it enciphers), the IP section data D22 to input are

enciphered -- as -- the 1- the 3rd encryption section 47A-47C is controlled.
[0058] The IP section data D22 for one packet given to 1st encryption section 47A through the encryption control section 45 at this time in this way After encryption processing was carried out based on 1st key data D19A used at the time of the encryption processing which was stored in 1st register 48A in the 1st encryption section 47A concerned, and to precede, Encryption processing is carried out based on 2nd key data D19B used for the 2nd register in 2nd encryption section 47B at the time of the encryption processing of which 48B storing was done, and to precede. After encryption processing is carried out based on 1st key data D19A stored in 1st register 48A in 3rd encryption section 47C after this, it is sent out to PAKETSUTAIZA 29 of the next step as above-mentioned encryption data D24 through the output section 49.
[0059] on the other hand, the encryption control section 45 is the timing to which the head detecting signal S10 was given based on the EN data D15 and the KA data D16 which are given from the 1st and 2nd data storage attaching parts 44A and 44B, and, in the case of EN=0 and KA=0 (neither encryption nor renewal of the key of encryption is carried out), does not encipher the IP section data D22 to input -- as -- the 1- the 3rd encryption section 47A-47C is controlled.
[0060] the IP section data D22 for one packet given to 1st encryption section 47A through the encryption control section 45 at this time in this way -- the 1- the 3rd encryption section 47A-47C is passed through, and it is sent out to PAKETSUTAIZA 29 of the next step as above-mentioned encryption data D24 through the output section 49 after this.
[0061] Thus, in this encryption processing section 28, it is made as [carry out / in each packet unit / the line of the on-off control of encryption and the updating control of the key in the case of enciphering], and is made as [perform / by this / to coincidence / encryption processing to two or more broadcast materials].
[0062] In actuation of the gestalt of this operation, and the configuration beyond effectiveness (4) In each data encoders 6A-6N for broadcast material encoding processing of this data-broadcasting system 1 When the data format of the broadcast material incorporated from read-out or the outside from the record playback section 7 is a DVB-SI format While this is sent out to a multiplexer 8 as it is, in being a section format or TCP/IP format of drawing 5 (B) After carrying out encryption processing if needed in the encryption processing section 28 and forming this into TS packet in PAKETSUTAIZA 29, it sends out to a multiplexer 8.

[0063] in this case, in these data encoders 6A-6N Data D1 A-D1N of the broadcast material incorporated from read-out or the outside from the record playback section 7, While adding the control header HD 5 which comes to include D2 A-D2N the EN data D15, the KA data D16, and the key data D19 like drawing 3 and packet-izing one by one Control of whether to these-encipher, since it is made as [perform / the control of whether to encipher which receives each / these / packet, an update process of the key in the case of enciphering, etc. / based on the EN data D15, the KA data D16, and the key data D19 which were stored in the corresponding control header HD 5], Updating control of the key in the case of enciphering etc. can be switched per packet, and can be performed.
[0064] In carrying out, with these data encoders 6A-6N, when [to write] data D1 A-D1N of each broadcast material and D2 A-D2N are incorporated from the record playback section 7 or the exterior to time sharing, the encryption processing to data D1 A-D1N of each broadcast material and D2 A-D2N can be switched one by one for every broadcast material, and can be performed.
[0065] Data D1 A-D1N of the broadcast material which was incorporated from read-out or the outside from the record playback section 7 according to the above configuration, Add the control header HD 5 which comes to contain the EN data D15 showing whether D2 A-D2N is enciphered, the KA data D16 showing whether a key is updated or not, and key data D19 grade, and it packet-izes one by one. By having been made to carry out encryption processing of the data D12 in the packet which corresponds based on the control header HD 5 concerned The data encoder which can make it possible to carry out switching encryption processing in each packet unit, and can perform encryption processing to data D1 A-D1N of two or more broadcast materials and D2 A-D2N to coincidence in this way is realizable.
[0066] (5) it is the gestalt of other operations -- in the gestalt of above-mentioned operation, although the case where this invention was applied to the data encoders 6A-6N was described, in addition to this, this invention is widely applicable to not only this but the data encoder for image voice, or various devices. Therefore, also when the objects which carry out encryption processing are material data other than data D1 A-D1N of a broadcast material, and D2 A-D2N, it can apply.
[0067] moreover, as a packet-ized means to add the EN data D15 which mean whether data D1 A-D1N of a broadcast material and D2 A-D2N are enciphered in the gestalt of above-mentioned operation, and to packet-ize per predetermined Although the case where the data-processing section 20 which

therefore performs header attached processing of the MAC header HD 2 with little ****** and section header HD3 grade etc. was applied to the software of the format conversion processings was described You may make it this invention form a packet-ized means in not only this but the data-processing section 20, and another object. Moreover, you may make it build a packet-ized means so that hardware processing may perform packet-ization.

[0068] Data D1 A-D1N of the broadcast material furthermore packet-ized in the gestalt of above-mentioned operation, Although the case where the encryption processing section 28 as an encryption means to encipher D12 if needed based on the EN data D15 contained in the control header HD 5 which corresponds for every packet was built like drawing 4 was described This invention can apply widely not only this but various configurations in addition to this.

[0069] Furthermore, it sets in the gestalt of above-mentioned operation. As 2nd encryption information showing whether the EN data D15 and the key in the case of enciphering are updated as 1st encryption information showing whether it enciphers or not Although the case where the key data D19 showing the ** KA data D16 and the key of new encryption were added to data D1 A-D1N of the broadcast material packet-ized as a control header HD 5 of a data format like drawing 3 and D12, respectively was described In addition to this, this invention can apply various formats widely as a format of not only this but the control header HD 5.

[0070] Furthermore in the gestalt of above-mentioned operation, the data encoders [6A-6N] data-processing section 20 is given from the record playback section 7. Or data D1 A-D1N of each incorporated broadcast material and D2 A-D2N are packet-ized in the magnitude of under 4 [Kbit] including the control header HD 5 from the outside. Although the case where the PCI control section 25 read the data of each [these] packet to the basis of control of the data-processing section 20 for every cluster through PCI bus 24 was described while carrying out sequential storing of this at each cluster of the record section of the memory 23 divided into every 4[Kbit] This invention may packet-be made toize data D1 A-D1N of not only this but each broadcast material, and D2 A-D2N in magnitude other than this, and can apply them widely a storing ways way other than this also as the storing approach for memory 23.

[0071] However, data D1 A-D1N of each broadcast material and D2 A-D2N are packet-ized including the control header HD 5 in the magnitude of under 4 [Kbit] (or the 1st predetermined magnitude other than this) in this way. While carrying out sequential storing of this at each cluster of the record section of the memory 23 divided into every 4[Kbit] So that the PCI control section 25 may read the data of each [these] packet to the basis of control of the data-processing section 20 for every cluster through PCI bus 24 Since the data of each packet can be read one by one only by making it increase to carrying out by 4 [Kbit] (or the 1st above-mentioned magnitude) every, and therefore specifying the address in memory 23 as it, read-out control of the data of each packet from memory 23 can be made to easy-ize.

[0072]

[Effect of the Invention] In the encryption equipment which enciphers the material data to input if needed as mentioned above according to this invention A packet-ized means to add the 1st encryption information showing whether material data are enciphered, and to packet-ize per predetermined, By having established an encryption means to encipher the packet-ized material data if needed based on the 1st encryption information which corresponds for every packet It can control per packet whether it enciphers or not and the encryption equipment of a simple configuration of that encryption processing of two or more material data can be carried out at coincidence can be realized in this way.

[0073] Moreover, according to this invention, the material data to input are set to the encryption approach enciphered if needed. The 1st step which adds the 1st encryption information showing whether material data are enciphered, and is packet-ized per predetermined, By having prepared the 2nd step which enciphers the packet-ized material data if needed based on the 1st encryption information which corresponds for every packet It can control per packet whether it enciphers or not and the encryption approach of a simple configuration of that encryption processing of two or more material data can be carried out at coincidence can be realized in this way.

[Translation done.]